United States Government Accountability Office

Report to Congressional Committees

February 2016

COUNTERFEIT PARTS

DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk

GAO-16-236

February 2016

COUNTERFEIT PARTS

DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk

GAO Highlights

Highlights of GAO-16-236, a report to congressional committees

Why GAO Did This Study

The DOD supply chain is vulnerable to the risk of counterfeit parts, which have the potential to delay missions and ultimately endanger service members. To effectively identify and mitigate this risk, DOD began requiring its agencies in 2013 and its contractors in 2014, to report data on suspect counterfeit parts. A Senate report included a provision for GAO to review DOD's efforts to secure its supply chain from counterfeit parts. This report examines, among other things, (1) the use of GIDEP to report counterfeits, (2) GIDEP's effectiveness as an early warning system, and (3) DOD's assessment of defense contractors' systems for detecting and avoiding counterfeits.

GAO analyzed data from GIDEP for fiscal years 2011 through 2015; reviewed DOD policies, procedures, and documents; and met with agency officials and seven selected contractors based on dollar value from contracts that included a new counterfeit clause.

What GAO Recommends

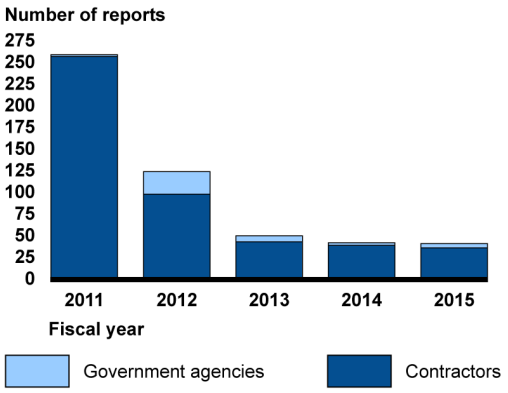
GAO recommends that DOD oversee its defense agencies' reporting efforts, develop standard processes for when to report a part as suspect counterfeit, establish guidance for when to limit access tor GIDEP reports, and clarify criteria to contractors for their detection systems. DOD agreed with the 3 recommendations on GIDEP reporting but partially agreed with the recommendation to clarify criteria, stating it did not agree with providing specific implementation details. GAO continues to believe clarifying criteria is important, which is different than specific implementation details.

View GAO-16-236. For more information, contact Marie Mak at (202) 512-4841 or MakM@gao.gov.

What GAO Found

Department of Defense (DOD) agencies and contractors submitted 526 suspect counterfeit parts reports in the Government-Industry Data Exchange Program (GIDEP) from fiscal years 2011 through 2015, submitted primarily by contractors. Defense agencies and contractor officials explained that congressional attention to counterfeit parts in 2011 and 2012 led to increased reporting, and that the lower number of reports in more recent years is partly the result of better practices to prevent the purchase of counterfeit parts.

Number of Suspect Counterfeit Reports for Fiscal Years 2011–2015



Source: GAO analysis of Government-Industry Data Exchange Program data. | GAO-16-236

Several aspects of DOD's implementation of its mandatory GIDEP reporting for suspect counterfeit parts have limited GIDEP's effectiveness as an early warning system.

- First, DOD is not conducting oversight to ensure that defense agencies are reporting as required. As a result, the Defense Logistics Agency (DLA), for example, may be underreporting suspect counterfeit parts in GIDEP.
- Second, there is no standardized process for establishing how much evidence is needed before reporting suspect counterfeit parts in GIDEP and DLA applies a significantly more stringent standard than, for example, the Navy. Consequently, reports may not be submitted in a timely manner.
- Third, defense agencies typically limit access of suspect counterfeit GIDEP reports to government agencies, so industry is not aware of the potential counterfeiting issues identified. DOD policy does not include guidance about when access to these reports should be limited.

All seven contractors GAO spoke with have established systems to detect and avoid counterfeit electronic parts; however, DOD has not finalized how these systems will be assessed. Contractors are seeking additional clarification on how to meet some of DOD's requirements. Until DOD clarifies criteria for contractors on how their systems will be evaluated, it cannot fully ensure these systems detect and avoid electronic counterfeit parts, as required.

Contents

Letter		1
	Background	3
	Defense Agencies and Contractors Are Submitting Fewer Counterfeit Parts Reports in GIDEP	10
	Aspects of Implementation Have Limited GIDEP's Effectiveness as an Early Warning System for Counterfeit Parts	12
	DOD Relies on Contractors to Implement Anti-Counterfeit Systems, but Has Yet to Develop Assessment Guidance DOD	21
	Counterfeit Detection Efforts Include Improving Testing and Traceability, Collaborating with Other Agencies, and Improving Purchasing Processes	27
	Conclusions	32
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	34
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	Number of Government-Industry Data Exchange Program (GIDEP) Reports by Role in Supply Chain of Entity Submitting Report (Fiscal Years 2011-2015)	40
Appendix III	Comments from the Department of Defense	41
Appendix IV	GAO Contact and Staff Acknowledgments	44

Figures

Figure 1: DOD Sources of Supply and Risk According to SAE Aerospace Standard 5553	4
Figure 2: Timeline of Federal Actions Related to GIDEP Reporting of Counterfeit Parts	7
Figure 3: Number of Government-Industry Data Exchange Program Suspect Counterfeit Reports for Fiscal Years 2011 – 2015	10
Figure 4: Varying Practices for Government-Industry Data Exchange Program Reporting	17

Figure 5: Comparison of Defense Contract Management Agency and Missile Defense Agency Contractor Evaluations for Counterfeit Detection and Avoidance Systems 25
Figure 6: Examples of Tests to Detect Suspect Counterfeit Electronic Parts 30

Abbreviations List

DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DLA	Defense Logistics Agency
DOD	Department of Defense
FAR	Federal Acquisition Regulation
GIDEP	Government-Industry Data Exchange Program
MDA	Missile Defense Agency
NASA	National Aeronautics and Space Administration
PDREP	Product Data Reporting and Evaluation Program
USD AT&L	Under Secretary of Defense for Acquisition, Technology, and Logistics

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 16, 2016

Congressional Committees

The Department of Defense (DOD) draws from a large network of global suppliers and, in fiscal year 2014, managed over 4.7 million parts that are used in, for example, communication and weapon systems, at a cost of over $96 billion. The existence of counterfeit parts in the DOD supply chain can, for example, delay missions, affect the integrity of systems, and ultimately endanger the lives of service members. Almost anything is at risk of being counterfeited, including microelectronics used in fighter jets and missile guidance systems, fasteners used in aircraft, and materials used in engine mounts. In response to this risk, in 2013, DOD created a Counterfeit Prevention Policy for department-wide action to mitigate the risk of counterfeit parts, which included steps to prevent the introduction of counterfeit materials into the supply chain, as well as testing and other means by which to detect materials that may have already entered it. DOD also issued regulations, as required by the 2012 National Defense Authorization Act, requiring that its personnel and contractors report suspected counterfeit electronic parts to a cooperative activity between government and industry for sharing technical information called the Government-Industry Data Exchange Program (GIDEP)—a program that allows government and industry participants to share information on nonconforming parts, including suspect counterfeit parts, via a web-based database—and that contractors develop and maintain systems to detect and avoid counterfeit electronic parts.

Congress has raised questions about DOD's ability to secure the supply chain and report on counterfeit or suspect counterfeit parts. The Senate Armed Services Committee report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2015 included a provision for GAO to review DOD's efforts to address vulnerabilities to counterfeit parts in its supply chain.[1] This report determines (1) the use of GIDEP to report suspect counterfeit parts, from fiscal years 2011 through 2015; (2) the effectiveness of GIDEP reporting as an early warning system for counterfeit parts; (3) the extent to which DOD has assessed defense

[1]S. Rep. No. 113-176, at 148 (2011).

contractors' systems for detecting and avoiding counterfeit parts; and (4) key ongoing efforts by selected government and industry organizations to improve the detection and reporting of counterfeit or suspect counterfeit parts.

To do this work, we examined laws and regulations regarding counterfeit parts, including section 818 of the 2012 National Defense Authorization Act, the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), as well as reviewed DOD counterfeit prevention policies and guidance relating to detecting and avoiding counterfeit parts. We reviewed the guidance on reporting counterfeit parts from the military services (the Departments of the Army, Air Force, and Navy) as well as from the Defense Contract Management Agency (DCMA), Defense Logistics Agency (DLA), and Missile Defense Agency (MDA) and interviewed officials about relevant policies and practices. We also analyzed data from GIDEP and the Product Data Reporting and Evaluation Program (PDREP) to determine the extent and limitations in reporting suspect and confirmed counterfeit parts for fiscal years 2011 through 2015. After interviewing GIDEP program officials and reviewing the entire GIDEP database and related documents, we determined that the data was sufficiently reliable for the purposes of this report. We selected seven contractors by identifying the top five prime contractors based on dollar value from contracts containing the 2014 DFARS clause for counterfeit detection and avoidance, as well as two additional major prime contractors. From each, we reviewed one sample contract as well as selected contractor procedures and systems for detecting and avoiding counterfeit parts; and identified and evaluated DOD's systems for monitoring contractor compliance with related regulations. We reviewed documents and met with officials from other selected federal agencies, such as the Department of Homeland Security and the National Aeronautics and Space Administration (NASA); as well as organizations including SAE International, Aerospace Industries Association, and the Independent Distributors of Electronics Association to obtain information about efforts to detect and avoid counterfeit parts. We visited DLA's Land and Maritime Division in Columbus, Ohio; where the agency maintains an electronic testing facility and an authentication program for microcircuits, and the product testing facilities at the Naval Surface Warfare Center in Crane, Indiana. We assessed DOD's policies, procedures and practices against criteria in *Standards for Internal Control*

in the Federal Government.[2] Appendix I provides a more detailed description of our scope and methodology.

We conducted this performance audit from January 2015 to February 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

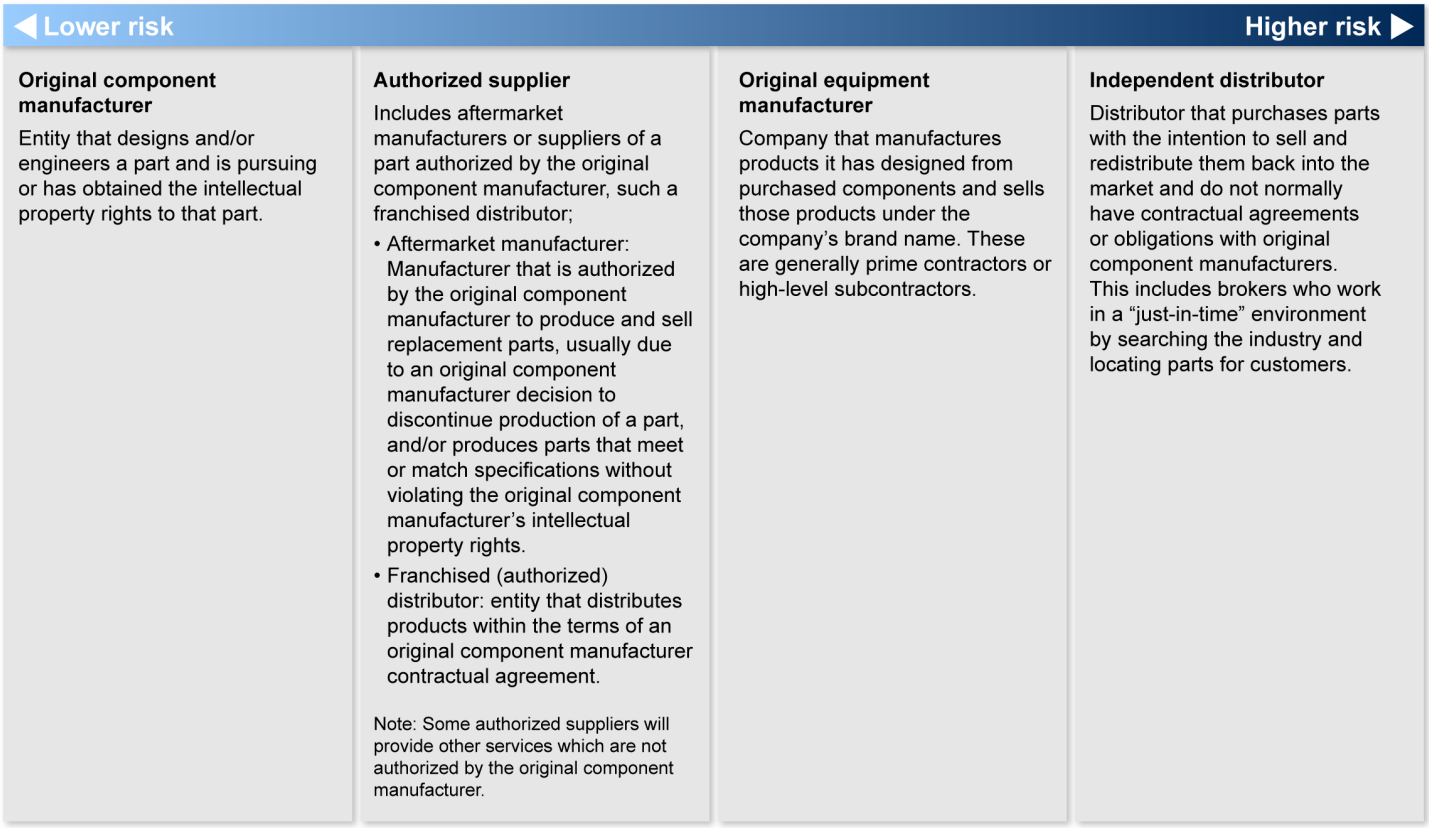
Background

DOD draws from a large number of suppliers in a global supply chain—in both the acquisition phase and throughout a system's operational and sustainment phases—providing multiple opportunities for the risk of counterfeit parts into these systems. DOD contractors rely on thousands of subcontractors and suppliers, including the original component manufacturers that assemble microcircuits and the mid-level manufacturers subcontracted to develop the individual subsystems that make up a complete system or supply. Once contractors deliver a system to the military services, DLA can play a critical role in its sustainment. For example, DLA is primarily responsible for logistical support for more than 2,400 weapon systems across the military services. As part of its sustainment functions, DLA provides approximately 90 percent of the military's repair parts. Also, as systems age, products required to support them may no longer be available from original component manufacturers, original equipment manufacturers or their authorized distributors. These products could be available from independent distributors, brokers, or aftermarket manufacturers; but these suppliers often have less traceability to the original source. DOD has adopted industry standards and continues to participate in government and industry groups that develop international standards for the aerospace and automotive industry, such as the SAE International's G-19 Committee. Specifically, in 2009 DOD adopted SAE International's Aerospace Standard 5553 Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition (AS5553) that includes definitions of the sources of supply for

[2]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

parts, and associated risk, which was updated in 2013 (as shown in figure 1).

Figure 1: DOD Sources of Supply and Risk According to SAE Aerospace Standard 5553



Source: GAO Summary of SAE International, AS5553A, Fraudulent/Counterfeit Electronic Parts Avoidance, Detection, Mitigation, and Disposition. Revised January 2013. | GAO-16-236

According to DLA officials, DLA does not use AS5553 because it is generally applied to system integrators, but uses other aerospace standards to govern its procurement of microelectronic parts from individual suppliers.[3] These standards emphasize the importance of purchasing parts from original component manufacturers or authorized

[3]SAE International, AS6174A, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel, Revised July 2014 and AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors, November 2012.

suppliers—when available—as the most effective method to avoid counterfeit parts. If purchasing a part from an independent distributor is necessary, the buyer should consider applying additional counterfeit mitigation methods, such as testing for product verification, based on the risk of the supplier and criticality of the part.

Over the past 6 years, GAO, Congress, and the Department of Commerce have issued reports on the existence of counterfeit parts in the DOD supply chain. In three reports since 2010, we have identified risks and challenges associated with counterfeit parts and counterfeit prevention at both DOD and NASA, including inconsistent definitions of counterfeit parts and poorly targeted quality control practices, as well as potential barriers to improvements to these practices.[4] In 2012, we created a fictitious company, and through it were able to report on the availability of suspect counterfeit electronic parts available for purchase from companies selling military-grade parts on the Internet. In our prior reports, we made a total of five recommendations for improvements. DOD has taken action to implement three of these recommendations, but neither DOD nor NASA have yet implemented the remaining two recommendations: on tracking the frequency with which parts with quality issues, including counterfeit parts, make their way into the supply chain; and on making that information available to Congress. In 2012, Senate investigators reported that approximately 1,800 instances of suspect counterfeit parts were identified by DLA, defense contractors and testers in the 2-year period from 2009 to 2010—before reporting suspect counterfeit parts in GIDEP became mandatory—and that the vast majority of those cases appeared to have gone unreported to DOD or criminal authorities.[5]

To enhance DOD's efforts to detect and avoid counterfeit electronic parts, Section 818 of the 2012 National Defense Authorization Act directed DOD to define suspect and confirmed counterfeit electronic parts, implement a

[4]GAO, *Defense Supplier Base: DOD Should Leverage Ongoing Initiatives In Developing Its Program to Mitigate Risk of Counterfeit Parts*, GAO-10-389, (Washington, D.C.: Mar. 29, 2010); GAO, *Space and Missile Acquisitions: Periodic Assessment Needed to Correct Parts Quality Problems in Major Programs*, GAO-11-404, (Washington, D.C.: Jun. 24, 2011); GAO, *DOD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*, GAO-12-375, (Washington, D.C.: Feb. 21, 2012).

[5]S. Rep. 112-167, Inquiry Into Counterfeit Electronic Parts in The Department of Defense Supply Chain (2012).

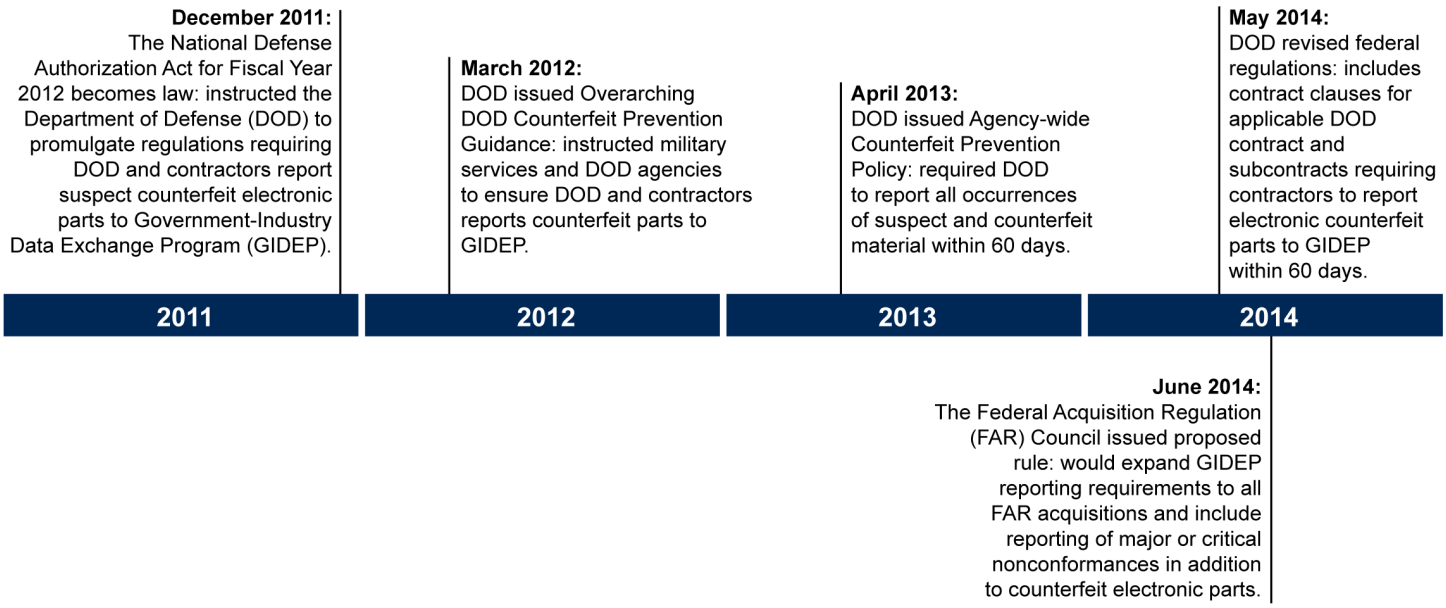
risk-based approach to mitigate the risk of counterfeit electronic parts, and use GIDEP to report counterfeit incidents.[6] It also included specific sections pertaining to DOD's supply chain—requiring certain DOD contractors to enhance their systems to detect and avoid counterfeit electronic parts, and to report all counterfeit and suspect counterfeit electronic parts in GIDEP within 60 days.[7] Finally, Section 818 required DOD to revise DFARS so that costs of rework or corrective action associated with a counterfeit electronic part supplied by certain contractors are not allowable under DOD contracts.[8] Figure 2 shows the timeline of congressional and DOD actions relating to counterfeit parts from 2011 to 2014.

[6]National Defense Authorization Act for Fiscal Year 2012. Pub. L. No. 112-81 (Dec 31, 2011).

[7]These requirements apply to prime contractors subject to cost accounting standards on acquisitions other than small business set-asides. The cost accounting standards are rules designed to ensure contractors consistently apply cost accounting practices to contracts with the government. These standards are prescribed by the cost accounting standards board under 41 U.S.C. § 1502.

[8]DOD implemented its cost principle that costs are not allowable unless 1) the contractor has an operational system to detect and avoid counterfeit parts that has been approved by DOD 2) the parts are government-furnished property, and 3) the contractor provided notice to the government within 60 days after the contract became aware of the suspected counterfeit part. DFARS § 231.205-71.

Figure 2: Timeline of Federal Actions Related to GIDEP Reporting of Counterfeit Parts



Source: PL 112-81, § 818; Memorandum for Secretaries of the Military Departments and Directors of the Defense Agencies, Overarching DOD Counterfeit Prevention Guidance (March 16, 2012); DODI 4140.67; 79 Federal Register 26092 (May 6, 2014); 79 Federal Register 33164 (June 10, 2014). | GAO-16-236

DOD issued its Counterfeit Prevention Policy in April 2013. The policy aims to 1) prevent the introduction of counterfeit materiel at any level of the DOD supply chain, including electronic parts; and 2) provide direction for anti-counterfeit measures for DOD weapon and information systems acquisition and sustainment to prevent the introduction of counterfeit materiel.[9] While the instructions in Section 818 to DOD are specifically applied to counterfeit electronic parts, the policy applies to all counterfeit materiel, not just electronic parts. DOD's Counterfeit Prevention Policy provides the following definitions for counterfeit items:

- Counterfeit materiel: an item that is an unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.

[9]Department of Defense Instruction 4140.67 DOD Counterfeit Prevention Counterfeit Prevention Policy, April 26, 2013. "Materiel" refers to military materials and equipment.

- Suspect counterfeit: materiel, items, or products in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel.

The Counterfeit Prevention Policy established roles and responsibilities for implementing DOD's anti-counterfeiting strategy as well as GIDEP reporting for counterfeit parts. Three offices within the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) have primary responsibility for counterfeit parts. First, the Assistant Secretary of Defense for Logistics and Materiel Readiness is designated as the primary point of contact office with the primary responsibility to implement, monitor, and continually develop DOD's anti-counterfeit strategy. Second, the Assistant Secretary of Defense for Research and Engineering, among other responsibilities, acts as the principal point of contact for GIDEP and is to determine and implement enhancements to GIDEP to expand its usefulness and robustness in anti-counterfeiting efforts in the DOD supply chain. Finally, the Director of Defense Procurement, Acquisition Policy, and Strategic Sourcing develops and modifies procurement policies, procedures, regulations, and guidance to support DOD's Counterfeit Prevention Policy.

DOD's Counterfeit Prevention Policy requires DOD component heads to report all occurrences of suspect and confirmed counterfeit parts in GIDEP, DOD's central reporting repository for suspect or confirmed counterfeit parts. Managed by DOD's Defense Standardization Program Office, GIDEP manages a web-based program that allows government and industry participants to share information on nonconforming parts, including but not limited to counterfeit parts (confirmed and suspected). Other types of information reported by GIDEP includes notices for when production of a part is about to be discontinued or when the attributes of parts, components, or materials have been changed by a manufacturer. A part that is found to be nonconforming is not necessarily counterfeit as counterfeit parts involve the intent to misrepresent the identity or pedigree of a part. DOD also uses the term "deficient" to have the same meaning as "nonconforming." The Policy requires the reporting of all occurrences of suspect and confirmed counterfeit materiel to (1) appropriate authorities, nonconformance reporting systems, and GIDEP within 60 calendar days; and (2) DOD criminal investigative organizations and other DOD law enforcement authorities at the earliest opportunity. It further states that when critical materiel is identified as suspect counterfeit, to expeditiously disseminate a notification to other DOD components to maintain weapon systems operational performance and preserve life or safety of operating personnel. According to several DOD

officials we spoke with, GIDEP is intended to be an early warning system. DOD military services and components also use two other systems to report nonconforming parts—the Product Data Reporting and Evaluation Program (PDREP) and the Joint Deficiency Reporting System.[10] In both systems, users can specifically categorize reported nonconforming parts as suspect counterfeit. As DOD's Counterfeit Prevention Policy mandates documenting all occurrences of suspect counterfeit parts in GIDEP, entries into these other systems do not fulfill the DOD reporting requirement. In May 2014, DOD revised the DFARS to require that contractors subject to cost accounting standards, when delivering electronic parts or supplies containing electronic parts, 1) report suspect and confirmed counterfeit electronic parts in GIDEP; and 2) have systems in place to detect and avoid counterfeit electronic parts. Additionally, the DFARS requires that prime contractors subject to the cost accounting standards flow down these requirements to their subcontractors, regardless of whether those subcontractors are subject to the cost accounting standards.[11] Prime contractors not subject to the cost accounting standards are not required to apply or flow down these requirements. The new counterfeit prevention policies supplement long-standing FAR contract quality requirements.[12]

[10]PDREP is managed by the Navy and is also used by the Army, DLA and the Defense Contract Management Agency. The Joint Deficiency Reporting System is used by the Air Force and Naval Air Systems Command.

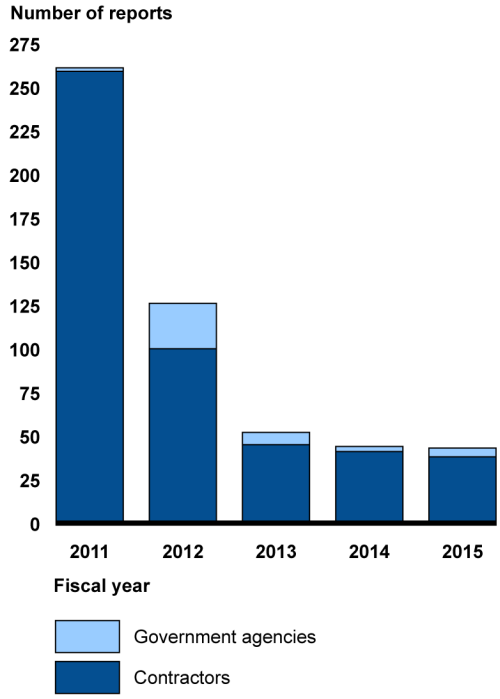
[11]The Office of Federal Procurement Policy's cost accounting standards cover a much broader range of requirements than just anti-counterfeit systems, and generally apply to those contractors receiving at least $50 million in government contracts. DFARS § 246.870-3(b) excludes small business set-aside contracts from the counterfeit prevention requirements, even if the contractor is subject to cost accounting standards.

[12]Under the FAR, contracts must include quality requirements, such as testing, inspection, and surveillance, necessary to protect the government's interest. The contractor is responsible for controlling the quality of its supplies or services while the government is responsible for contract quality assurance. Agencies have wide latitude to adjust quality assurance requirements according to the type of acquisition. The new DFARS counterfeit detection and avoidance policies provide more specific quality requirements. FAR §§ 46.102(a); 46.103(a); 46.105(a); 46.101; 46.401(a).

Defense Agencies and Contractors Are Submitting Fewer Counterfeit Parts Reports in GIDEP

Defense contractors and agencies are submitting counterfeit parts reports, but fewer reports have been submitted to GIDEP since DOD implemented its Counterfeit Prevention Policy and reporting requirements in 2013. For fiscal years 2011 through 2015, we found that 526 reports of suspect counterfeit parts were entered in GIDEP, over 90 percent of which were submitted by contractors.[13] Figure 3 shows the number of reports submitted by contractors and government agencies in each fiscal year.

Figure 3: Number of Government-Industry Data Exchange Program Suspect Counterfeit Reports for Fiscal Years 2011 – 2015



Source: GAO analysis of Government-Industry Data Exchange Program data. | GAO-16-236

[13]We did not include failure analysis reports – a particular GIDEP report type that addresses the root cause of part failures or suitability – in our analysis because GIDEP no longer identifies them as counterfeit parts reports for future submissions, in part because they generally do not include the information – such as supplier names – industry and government entities needs to manage the risks of counterfeit parts.

Most of these reports were submitted in 2011 and 2012, when some DOD and contractor officials we spoke with said that congressional attention to counterfeit parts prompted contractors to examine their inventory and identify previously undetected counterfeit parts. In addition, there was an amnesty period in early fiscal year 2011 when suspect counterfeit parts reports could be submitted without naming a supplier, which DOD officials said led to temporarily increased reporting, mostly from distributors who have submitted few reports since. In more recent years, defense agencies and contractors we met with stated that they have encountered counterfeit parts less frequently in the DOD supply chain, in part, because they are applying more stringent standards about which independent distributors they rely on for parts that cannot be acquired directly from the original manufacturer.

While the names of the suppliers can be identified in GIDEP reports, almost half of 526 GIDEP reports in our analysis did not include the name of the supplier for the parts in question. Further, the reports do not always indicate the original source from whom the supplier purchased the counterfeit part, which could be further down the supply chain and may or may not be known by the entity submitting the report. At our request, GIDEP staff categorized the suppliers identified in counterfeit parts reports issued in fiscal years 2011 through 2015 by their role in the supply chain, based on their personal knowledge and industry expertise, and we conducted analysis based on these classifications.[14] In the 296 reports that contained supplier information, 319 unique suppliers were named.[15] Of these, 88 percent were classified by GIDEP staff as independent distributors and 10 percent were classified as midlevel manufacturers. One independent distributor was named in 30 different GIDEP reports, all of which were submitted by one original equipment manufacturer within a 7-month period.

GIDEP staff also provided classifications for the entities that submitted GIDEP reports by their role in the supply chain, upon which we based our analysis. From fiscal years 2011 through 2015, we found that nearly 40 percent of suspect counterfeit parts reports—207 of 526—were

[14]GIDEP does not classify entities by their role in the supply chain. To categorize entities that submitted counterfeit parts reports in GIDEP, we asked GIDEP staff to provide these classifications but we could not independently verify them.

[15]Some GIDEP reports name multiple suppliers.

submitted by independent distributors, with three companies submitting 103 reports. In addition, one-third of all suspect counterfeit GIDEP reports—178 of 526—were submitted by original equipment manufacturers, with 122 of these 178 reports submitted by two manufacturers, while government agencies submitted only 43 reports. DOD submitted 40 of 43 government reports, with the Navy submitting more than half of these. See appendix II for additional details of reports by role of reporting entity in the supply chain.

The Army, the Air Force and MDA did not submit any suspect counterfeit GIDEP reports in this period. Air Force officials explained that they have relied on their contractors to submit reports because they have the best knowledge of how and where the counterfeit part was procured. Similarly, officials from the Army and MDA also said that their contractors have submitted suspect counterfeit GIDEP reports related to parts procured for Army and MDA products. Specifically, MDA officials said that their contractors submitted five of the GIDEP reports we reviewed, some of which involved parts detected due to concerns raised by MDA. DLA officials also noted that they encourage contractors and subcontractors to submit reports when counterfeit parts are encountered. However, according to DOD officials, most of DLA's contractors are not large enough to follow cost accounting standards and therefore are not bound by the GIDEP reporting requirement in the DFARS. To address this, defense officials stated that DLA requires any company participating in one of its qualified supplier programs to report in GIDEP.

Aspects of Implementation Have Limited GIDEP's Effectiveness as an Early Warning System for Counterfeit Parts

Several aspects of DOD's implementation of its mandatory reporting requirement for suspect counterfeit parts in GIDEP have limited GIDEP's effectiveness as an early warning system to prevent counterfeit parts from entering the defense supply chain. First, DOD has not established an oversight function to ensure that defense agencies are reporting suspect counterfeit parts as required. As a result, for example, reporting practices at DLA do not conform to either DOD- or DLA-level reporting policies and it is likely that DLA is not reporting all of the suspect counterfeit parts detected in GIDEP as suspect counterfeit parts. Second, there is not a standardized process for establishing how much evidence is needed before reporting suspect counterfeit parts in GIDEP. We found that defense agencies and contractors have used different practices for determining when to report a part as suspect counterfeit and DLA applies a significantly more stringent standard than other defense agencies and contractors we reviewed. As a result, reports may not be submitted in a timely manner. Third, defense agencies typically limit access of suspect

counterfeit GIDEP reports to government agencies, so industry is not aware of the potential counterfeiting issues identified. DOD's Counterfeit Prevention Policy does not include guidance about when limiting access to suspect counterfeit parts GIDEP reports is appropriate. *Standards for Internal Control in the Federal Government* call for information to be recorded and communicated to others, such as stakeholders who need it, to help the agency achieve its goals. These standards also state that control activities should be in place to help ensure that management's directives are carried out, such as ensuring completeness and accuracy of information processing.[16]

Limited Department-Level Oversight Leads to Uncertainty about Completeness of GIDEP Reporting

DOD has not provided adequate department-level oversight to ensure that all defense agencies are reporting in GIDEP as required and, as a result, it is likely that defense agencies—particularly DLA—are not reporting all of the suspect counterfeit parts they detect in GIDEP as suspect counterfeit. *Standards for Internal Control in the Federal Government* call for reviews by management at the functional or activity level to compare actual performance to planned or expected performance and analyze significant differences.[17] Completeness and timeliness of GIDEP reporting relies on DOD ensuring that reporting practices align with established Counterfeit Prevention Policy. According to a senior USD AT&L official, GIDEP staff do not play a role in overseeing and monitoring whether defense agencies and contractors are meeting reporting requirements. DOD policy does not provide for an oversight role to ensure that reporting of counterfeit parts is tracked. The senior USD AT&L official explained that the department has taken a decentralized approach to implementing GIDEP reporting requirements, depending on the components to provide additional guidance and oversight. While defense agencies generally each have a central point person overseeing use of GIDEP, DOD does not oversee GIDEP reporting at a department-wide level. According to DOD's Counterfeit Prevention Policy, three entities within USD AT&L share responsibilities for DOD's anti-counterfeiting efforts. The senior USD AT&L official stated that certain GIDEP oversight functions, such as oversight of reporting by DOD agencies, may fall between the responsibilities of these organizations.

[16]GAO/AIMD-00-21.3.1.

[17]GAO/AIMD-00-21.3.1.

Moreover, defense officials have not analyzed or provided oversight of defense agencies' compliance with GIDEP reporting requirements, monitoring only whether agencies have established their own policies. A senior USD AT&L official responsible for counterfeit prevention policy we spoke with was not aware of DLA's low level of reporting and has not analyzed the reasons for it in light of DLA's central role in procuring parts for DOD. Specifically, this official said that USD AT&L has not conducted analysis that shows that DLA submitted very few reports in recent years. As a result of DOD's decentralized approach and lack of department-level oversight, the department cannot ensure that GIDEP data accurately reflect the extent to which suspect counterfeit parts have been identified by defense agencies.

DLA plays a central role in procuring parts to sustain existing weapon systems. Navy and Air Force officials we spoke with noted that they do not typically purchase parts directly from suppliers, so they would expect counterfeit parts to be reported by their defense contractors or DLA. However, DLA submitted only nine suspect counterfeit GIDEP reports in fiscal years 2011 through 2015, with none submitted in 2014 and just one in 2015. DLA officials described instances where parts were identified as potentially suspect counterfeit, but these were reported in GIDEP as nonconforming parts, not suspect counterfeit. While this step provides GIDEP users with notice that parts did not meet contract specifications and may present safety problems, it does not inform users about potential counterfeiting concerns.

In another example, in 2012, the Air Force did not report a debarred subcontractor in GIDEP for supplying counterfeit electronics components, even after the investigation was made public.[18] Although Air Force officials stated that its prime contractor submitted related suspect counterfeit GIDEP reports about some parts, these reports did not include the name of the debarred subcontractor; rather they listed only the independent distributor that the parts were sold through. Without a GIDEP report that included critical information about the original source of suspect counterfeit parts, other defense agencies and contractors may not have the information necessary to raise their awareness of the

[18]Debarment is an administrative remedy that agencies may use to protect the government's interests by excluding individuals, contractors, and grantees from receiving federal contracts, grants, and other forms of financial assistance based on various types of misconduct.

problem or to check whether other distributors also sold parts from that same source.

Further, DOD officials told us that not all suspect counterfeit parts that are reported to other data sources are reported in GIDEP as suspect counterfeit. Specifically, PDREP—the Navy's system for reporting supplier performance and quality information used across several defense agencies—allows the entity that submits a report about a nonconforming part to identify the part as suspect counterfeit. According to DOD policy, it is then the responsibility of a specific agency identified in PDREP to determine whether to report in GIDEP, which is possible through an automated function within PDREP. We found 268 PDREP reports labeled as suspect counterfeit parts by various DOD entities between October 2010 and August 2015.[19] However, only 10—or 4 percent—are clearly documented as having been reported in GIDEP. While defense agency and contractor officials explained that there are instances where an initial suspicion of counterfeiting is quickly proven incorrect, defense officials also stated that at least some parts identified in PDREP as potentially counterfeit should be reported in GIDEP but are not. Navy officials noted that this is particularly common when DLA is responsible for resolving the claims. For example, DLA created a parts quality report in PDREP, coded the parts report as suspect counterfeit, and tested the parts at its product testing and evaluation program. The parts failed visual and dimensional test requirements, but were not reported in GIDEP as suspect counterfeit. DLA was the agency responsible for determining whether to report in GIDEP for 148 of the 268 PDREP reports we reviewed that were labeled as suspect counterfeit. However, DLA submitted only one of the related GIDEP reports we identified.

In our review, we found that another source of information about suspect counterfeit parts and their suppliers, ERAI, had significantly more suspect counterfeit reports than GIDEP, further calling into question GIDEP's completeness. ERAI—a company that monitors, investigates and reports issues affecting the global electronics supply chain—provides paying members from government and industry with access to a database with reports of nonconforming parts and their suppliers. According to ERAI,

[19]We did not include PDREP reports issued in September 2015 in our analysis because we conducted our analysis prior to the end of fiscal year 2015.

most of its members are independent brokers, but also includes original equipment manufacturers and government users. According to ERAI's data its users report more suspect counterfeit parts than are reported in GIDEP. For example, from 2011 through 2015, over 4,000 reports of suspect counterfeit electrical, electronic, and electromechanical parts were submitted to ERAI, over 7 times the amount of suspect counterfeit reports for all types of parts submitted in GIDEP during the same period.[20] ERAI and agency officials largely attribute this high number to the fact that reports in ERAI are submitted anonymously. While ERAI includes reports about commercial and defense industry suppliers, an ERAI official noted that both sectors often rely on the same pool of suppliers.

DOD Lacks a Standardized Process for Determining When to Report Suspect Counterfeit Parts in GIDEP

There is no standardized process for establishing how much evidence is needed before reporting suspect counterfeit parts in GIDEP, and DLA applies a more stringent standard than other defense agencies and contractors we reviewed. When suspect counterfeit parts are discovered, we found that defense agencies and contractors generally take additional steps to establish reasonable certainty that parts are counterfeit before submitting suspect counterfeit GIDEP reports, although practices for making this determination differ and therefore take varying amounts of time. We found that some of the defense agencies and contractors we reviewed have practices for reporting parts as suspect counterfeit in GIDEP within the 60-day reporting period, but that DLA's practices can take significantly longer to complete.

According to the GIDEP operations manual, reports should be submitted no more than 60 days from the time of discovery to preclude further loss to government and industry users. In addition, the objective of GIDEP reports, including suspect counterfeit parts reports, is to preclude the integration of these items into government and industry systems and inventory.[21] Moreover, DOD's 2013 Counterfeit Prevention Policy states that it is DOD's policy to make information about counterfeiting accessible at all levels of the DOD supply chain as a method to prevent further counterfeiting.[22] DOD and industry officials noted that timely reporting of

[20]We did not assess the reliability of ERAI's data.

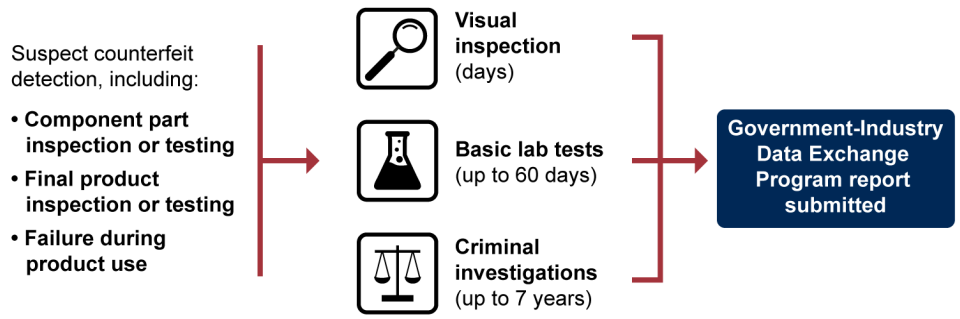
[21]GIDEP Operations Manual, Chapter 7. para. 7.3 (2015).

[22]DOD Instruction 4140.67, DOD Counterfeit Prevention Policy, para. 3.d (April 26, 2013).

suspect counterfeit parts to GIDEP is critical to using the system as an early warning system. For example, one USD AT&L official stated that DOD's goal for GIDEP reporting is to get information about suspect counterfeit parts out as early and as far down the supply chain as possible. However, DOD and industry officials told us they were concerned that GIDEP could not be relied upon to meet this goal if suspect counterfeit parts reports were not made available to industry in a timely and comprehensive manner.

Defense agencies and contractors have varying practices for establishing reasonable certainty after a suspect counterfeit part is discovered. Some DOD officials stated that confirming whether a part is indeed counterfeit requires 1) verification by the manufacturer of that part, 2) completion of a criminal investigation, or 3) comprehensive testing that uncovers multiple strong physical counterfeit indicators. Figure 4 illustrates varying practices for determining whether to submit a GIDEP report.

Figure 4: Varying Practices for Government-Industry Data Exchange Program Reporting



Source: GAO analysis of defense agency and contractor documents and testimony. | GAO-16-236

Some defense agencies and contractors have established practices that allow them to meet GIDEP's 60-day reporting requirements. For example, one defense contractor told us it issues a GIDEP report as soon as it has any indication that a part may be counterfeit and another defense contractor told us it conducts routine laboratory tests on any suspect counterfeit parts, which it said can usually be completed within GIDEP's 60-day reporting requirement. The Naval Surface Warfare Center Crane has established a standardized process for evaluating parts suspected of being counterfeit. Specifically, it conducts preliminary engineering investigations to confirm that a part is suspect counterfeit, conducts detailed analysis to calculate scores that measure how certain they are of

their suspicions, and then submits GIDEP reports if appropriate. Navy officials explained that they use a scoring system that weights different types of tests and other information differently, depending on their reliability in determining whether a part is counterfeit. The scoring system totals up an overall point-value for an assessment, and officials said they report to GIDEP once the assessment reaches a certain threshold. Navy officials stated that, in general, this process can take from a week to a month, but they can generally meet GIDEP's 60-day reporting requirement.

In contrast, DLA officials said that when DLA first identifies a part as suspect counterfeit, it initially submits a GIDEP report identifying it simply as nonconforming—rather than suspect counterfeit—and with access limited to government use only. It then refers the allegation for a full criminal investigation and, if the investigation confirms that a part is counterfeit, DLA may amend or initiate a new GIDEP report that labels it as counterfeit—however, these investigations can take up to 5 to 7 years. Some defense agency officials said that early GIDEP reporting could interfere with criminal investigations and that reporting needs to wait until indictments are completed so as not to jeopardize the investigation. Officials from the Defense Criminal Investigative Service described certain instances when law enforcement activities may delay releasing suspect counterfeit GIDEP reports, including cases where a covert investigation is underway or there are activities related to a grand jury. However, they noted that these instances are uncommon and that disseminating information takes priority in the event that a suspect counterfeit part poses a health or safety risk. Defense Criminal Investigative Service officials stated that they follow DOD's written procedures for coordination with DOD components.[23]

DLA's practice of not reporting parts to GIDEP as suspect counterfeit until a full investigation has been completed does not align with DLA's policies that require all instances of suspect and confirmed counterfeit parts be documented in GIDEP. According to DLA, 19,000 personnel are trained annually on DLA's counterfeit prevention procedures. However, one DLA official we spoke with acknowledged that although he was trained about the DLA procedures that require them to report any suspect parts, he said

[23]Defense of Defense Instruction 7050.05, "Corruption of Remedies for Fraud and Corruption Related to Procurement Activities," May 12, 2014.

that he disagreed with the policy and that GIDEP should only contain confirmed counterfeit parts data.

Some defense contractors are reluctant to allege that a supplier has delivered counterfeit parts without establishing certainty due to concerns about damaging relationships with suppliers up to and including the possibility of being sued if their claims damage the supplier's business. While the 2012 National Defense Authorization Act included language protecting contractors that made a reasonable effort to determine whether a part contained counterfeit or suspect counterfeit parts from civil liability for reporting, contractors we spoke with differed on the extent to which they believe those protections are adequate to protect their financial interests. Some contractors stated that they believe reporting a suspect counterfeit part in GIDEP may leave the contractor open to legal action if the part is determined to be genuine. To address similar concerns, DOD officials said GIDEP established an amnesty period in late 2010 when suspect counterfeit parts reports did not need to include the name of the supplier. Although this temporarily increased reporting, some contractor officials told us that reports without supplier information are difficult to act upon because this information is often necessary for identifying parts in their inventories. As an alternative, contractor officials said it would help alleviate these concerns if GIDEP reporting provided anonymity for the entity submitting the reports, either by having the government submit the report on their behalf or by masking the name of the submitter in the publicly released report.

Air Force and GIDEP officials told us that contractors involved in developing products that will be launched or deployed into space have worked with GIDEP to establish a separate, private system for early reporting of nonconforming parts based on limited information, due to the greater risk associated with incorporating counterfeit or faulty parts in space systems. Some defense officials we spoke with noted that a tiered reporting system—for instance indicating that an early report is based on preliminary information while subsequent updates could be based on a more complete investigation—would increase comfort with reporting suspect counterfeit parts based on limited testing information.

Standards for Internal Control in the Federal Government state that management should establish procedures that are effective in

accomplishing agency objectives.[24] In the absence of such procedures for determining when to submit suspect counterfeit parts reports in GIDEP, DOD is unable to ensure that the information is submitted in a timely manner, undermining GIDEP's usefulness as an early warning system.

Industry Is Concerned about Lack of Access to Government Issued GIDEP Reports

Industry was the biggest user of suspect counterfeit part GIDEP reports issued in fiscal years 2011 through 2015, with industry users responsible for 96 percent of all suspect counterfeit GIDEP report downloads. Similarly, as noted previously, 90 percent of the reports were submitted by industry. However, industry officials expressed frustration that access to government-submitted GIDEP reports is often limited to government agencies. As a result, contractors are not able to read them and take responsive actions. We found that most of the suspect counterfeit GIDEP reports submitted by government agencies were not available to industry GIDEP participants. Specifically, 29 of 43 suspect counterfeit GIDEP reports submitted by government agencies in fiscal years 2011 through 2015 were issued with limited access—only viewable by government agencies. In addition, while DOD has other internal information systems that capture information about suspect counterfeit parts, such as PDREP and a department-wide notification system, none of these are fully available to industry participants in the supply chain.

Industry officials told us that, while the quality of GIDEP reports varies, they depend on GIDEP reports because they generally include the most robust information about counterfeit parts among data sources available to them. For instance, industry officials stated that it is very helpful to know the source which supplied a counterfeit part to assess the potential impact of a counterfeit part in the supply chain, but this information is generally not available from other sources. Counterfeit parts GIDEP reports are most useful if they are made available as early as possible, so contractors can take necessary actions before they also purchase the same parts. *Standards for Internal Control in the Federal Government* call for information and communications to be recorded and communicated to others, such as stakeholders who need it, to help the agency achieve its goals.[25] DOD's Counterfeit Prevention Policy does not include guidance

[24]GAO/AIMD-00-21.3.1.

[25]GAO/AIMD-00-21.3.1.

about when limiting access to suspect counterfeit parts GIDEP reports is appropriate.

While industry officials told us that individual suspect counterfeit GIDEP reports are useful, they also said it is difficult to analyze GIDEP's data, due to several limitations. For example, they said that the GIDEP information system is more than 15 years old and relies on antiquated technology. In addition, the system is primarily based on downloads of full documents, which limits users' ability to search and analyze reports. According to a senior USD AT&L official, GIDEP staff conduct their own analysis, but do not disseminate all of this information outside their office. GIDEP officials are developing plans to modernize the GIDEP system to accommodate potential access by allies and foreign partners, and address these known limitations. According to the head of GIDEP, several improvements are needed, including updating the website, improving search functions, and improving the capability to extract data for analysis. However, this official stated that no formal decisions have been made as to whether to fund any of these improvements. In addition, a proposed FAR rule, if finalized, would expand the GIDEP reporting requirement to all government agencies' contractors and would require reporting of all nonconforming parts. However, because GIDEP staff reviews each submitted report individually, concerns exist on whether GIDEP staff and technology could handle a large surge in reporting.

DOD Relies on Contractors to Implement Anti-Counterfeit Systems, but Has Yet to Develop Assessment Guidance

DOD's Counterfeit Prevention Policy depends on coordinated action by both DOD agencies and prime contractors. The DFARS requires prime contractors subject to the cost accounting standards to have anti-counterfeit systems in place; however, the guidance and criteria for DOD to assess these systems are still under development. Consequently, defense contractors have expressed uncertainty about what steps are required of them and which approaches will be deemed adequate by DOD. DOD is working with industry to develop and clarify these standards to avoid and detect counterfeit electronic parts within the defense supply chain. Until the final guidance on how DOD will assess contractors' systems for detecting and avoiding counterfeit electronic parts is in place, DOD will be unable to fully ensure that these anti-counterfeit systems address what is required in the DFARS for counterfeit electronic parts.

DOD Is Incorporating Counterfeit Parts Policy into Existing Monitoring Activities

DOD's Counterfeit Prevention Policy depends on coordinated action by both DOD agencies and prime contractors. Consequently, the regulations and policies lay out requirements for both public and private entities involved in defense contracting, as well as DOD's responsibilities for overseeing these requirements. Section 818 of the National Defense Authorization Act of 2012 required DOD to implement a program to enhance contractor detection and avoidance of counterfeit electronic parts. Section 818 required the DOD program apply not only to its prime contractors subject to the cost accounting standards, but also to all their subcontractors, regardless of whether the subcontractors were subject to the cost accounting standards. DOD relies heavily on contractors to prevent the introduction of counterfeit materiel into the DOD supply chain, and oversight of these contractor programs to detect and avoid counterfeit electronic parts was delegated to the DCMA. Additionally, Section 818 deems the costs of counterfeit electronic parts and suspect counterfeit electronic parts, including any rework or corrective action required to remedy their use, unallowable, providing incentives for contractors to ensure that they detect counterfeit and suspect counterfeit electronic parts.

When delegated by the contracting officer, DCMA quality assurance and contracting staff oversee a prime contractor's purchasing systems, which can include reviews of the contractor's counterfeit electronic part detection and avoidance system. During these reviews, DCMA staff examine 12 categories of prime contractor compliance—such as reporting and quarantining suspect counterfeit and counterfeit electronic parts—and ensure that they have effective counterfeit detection and avoidance systems. DCMA's initial efforts to assess the status of contractors' counterfeit detection and avoidance systems have begun to identify areas that might require increased oversight. For example, DCMA data as of fall 2015 indicate that approximately 80 percent of suppliers it reviews have processes in place for maintaining part traceability and that approximately 70 percent have processes in place for reporting and quarantining counterfeit or suspect counterfeit electronic parts. DCMA continues to incorporate compliance with counterfeit detection and avoidance in its contractor purchasing system review instruction, but has not yet reviewed any individual contracts for compliance with the r counterfeit electronic parts requirement since it was imposed in 2014.

Selected Contractors Worked with DOD to Implement Anti-Counterfeit Systems, but DOD Assessment Criteria Is Lacking

Based on our discussions with selected contractors, we found that each of the seven contractors has systems in place to detect and avoid counterfeit parts. These included actions such as: screening of GIDEP and other data sources to identify potential threats of counterfeit parts, using risk analyses to assess the appropriate level of scrutiny for a part, and narrowing the list of suppliers being treated as authorized sources of parts. For at least three of the selected contractors, these business processes predated the DFARS requirement that they have such processes. However, all seven contractors have provided some degree of input to DOD on changes to the laws or additional clarity in guidance that they would like to see.

Collaboration between DOD and industry on proposed rules and policies for the detection and avoidance of counterfeit parts has played an important role in ensuring effective action on both sides. DOD has hosted numerous meetings and interactions between government and industry over the last four years concerning the 2012 National Defense Authorization Act language on counterfeit electronic parts and the development of rules and regulations surrounding it. These have included public meetings by DOD to obtain views on the rulemaking, briefings with DCMA on the adequacy of plans for the detection and avoidance of counterfeit parts, and counterfeit parts enforcement forums with Departments of Justice and Homeland Security. DOD officials stated that these meetings are valuable for crafting DOD policy and setting industry expectations. The contractors we spoke with had all participated in these interactions in some capacity, either directly or through an industry organization, and often both. Some contractors provided both positive and negative views on DOD's engagement, but their responses generally suggest that DOD was listening to the industry, and responding as appropriate.[26]

Despite contractors' efforts to work with DOD in developing and commenting on the rules and regulations, several have expressed concern on the lack of clear criteria on elements such as traceability and testing. They generally indicated that the lack of clear assessment criteria from DCMA on what steps prime contractors should take to meet the requirements in each of the 12 categories complicated their efforts to

[26]Because this was a small, non-generalizable sample of prime contractors, these views should not be taken as representative of the defense industry as a whole.

ensure that their counterfeit detection and avoidance systems meet DFARS requirements. For example, one contractor stated that it would like to use third-party testing of certain electronic parts, but without clear guidance from DCMA on whether this activity would meet certain counterfeit avoidance requirements and which test facilities may be approved for use, it is harder to invest in appropriate solutions. The DFARS states that DOD is to review the acceptability of contractors' counterfeit electronic part detection and avoidance systems.[27] However, according to DCMA officials, DCMA's current guidance is intended to provide flexibility for prime contractors on how they can address each of the 12 categories on which they will be assessed, rather than identify specific procedures.

During our review, DCMA indicated that it is revising its January 2014 instruction on contractor purchasing system reviews to include criteria for assessing counterfeit detection and avoidance systems. In addition, DCMA is updating its counterfeit mitigation instruction to address counterfeit detection and mitigation for DCMA analysts to use while conducting their reviews. *Standards for Internal Control in the Federal Government* state that for an entity to run and control its operations, it must have relevant, reliable, and timely communications relating to internal as well as external events.[28] Both the instruction and the guidebook are intended to assist the DCMA workforce to adequately assess contractor performance to the requirements, but do not provide clarification for industry.

In contrast to DCMA, clarification for industry on how to effectively meet the DFARS criteria has been developed elsewhere in DOD to support counterfeit detection and avoidance in high risk programs. Specifically, MDA provides a checklist to its contractors that goes into greater detail and provides clarity on what MDA will assess as an adequate counterfeit detection and avoidance system. For example, DCMA's checklist generally asks about the flow down of counterfeit avoidance and detection requirements to subcontractors, while MDA's checklist provides the specific steps required to verify flow down. Figure 5 contrasts DCMA and MDA's worksheets for evaluating contractors' counterfeit avoidance and detection systems. Without more detailed clarification on how to meet

[27]DFARS § 252.246-7007(d).

[28]GAO/AIMD-00-21.3.1.

DCMA criteria, such as that presented in the MDA checklist, contractors cannot be certain how to implement systems that will pass DCMA review.

Figure 5: Comparison of Defense Contract Management Agency and Missile Defense Agency Contractor Evaluations for Counterfeit Detection and Avoidance Systems

Defense Contract Management Agency checklist

Does the Contractor's counterfeit part detection and avoidance system include risk-based policies and procedures that address, at a minimum, the following:			
EXAMPLE 1. The training of personnel.	Y	INTERNAL INST / POLICIES as noted	There is no evidence that the contractor/supplier(s) processes are implemented.
7. Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit?			
8. Design, operation, and maintenance of systems to detect and avoid counterfeit and suspect counterfeit parts?			
9 . Flow down of counterfeit avoidance and detection requirements?			

Missile Defense Agency checklist

					Rating Guidance (0 to 5)				
	Subcontractor Flow Down Verification			0%	0	1	2	5	Guidance
I1	Does the contractor maintain a subcontractor compliance assessment schedule for all suppliers of mission and safety critical hardware?	10		0.0	No assessment schedule is maintained.	A schedule is maintained, but there are no firm dates, or assessment dates are not being met.	A schedule is maintained, and there are firm dates. Contractor is behind schedule.	A schedule is maintained per process, and there are firm dates. Contractor is on shedule. Corrective actions are being closed promptly. Assessment summaries are readily available and used to improve the process.	Contractor should have an MDA-approved subcontractor assessment schedule for ensuring flow down of anti-counterfeit requirements to lower tiers. Progress of assessments, including percent completion, should be readily providable.
I2	Does the contractor have documented criteria for defining suppliers of mission and safety critical hardware?	5		0.0	No criteria for defining critical suppliers.		There are general undocumented criteria for identifying critical suppliers.	There are defined criteria for identifying mission and safety critical suppliers.	For Award Fee compliance, contractor should have an MDA-approved subcontractor assessment schedule for meeting this question. Provide progress of assessments..
I3	How well does the contractor flow the supplier approva items in Section B to the critical subcontractors?	3		0.0	None of the supplier selection requirements are flowed down.	The subcontractor must maintain an Approved Supplier Listing and nothing else.	At least three of the Section B questions are flowed as requirements, but customer notification is not one of them.	All of the Section B questions are flowed as requirements.	Section 3.6.7.1 of the MDA PMAP details the requirements.

Ratings 3 and 4 are removed.

Source: GAO excerpt of defense agency documents. | GAO-16-236

Contractors Provided Different Perspectives on Applicability and Coverage of Counterfeit Part Regulations

Each of the seven selected contractors we met with told us, and we confirmed through selected contract review, that it was required to flow down—or ensure its subcontractors' contracts included—the DFARS clause requiring subcontractors to have systems to detect and avoid counterfeit electronic parts. These contractors each explained their policies or processes for flowing down these requirements and told us that they use a risk-based approach to oversee subcontractors, including those at lower tiers. These risk-based approaches varied from one contractor to another, but generally involved a preference for purchasing

from original part manufacturers or other reliable suppliers, for instance those authorized by the original part manufacturers, and applying greater scrutiny to parts purchased from other sources, and expecting or requiring their subcontractors to do the same.

However, we found disparity on the interpretation of this DFARS clause flowing counterfeit electronic parts regulations down to subcontractors. Specifically, although three of the contractors we spoke with identified no difficulties in effectively passing down these requirements to their subcontractors, four others discussed varying degrees of resistance by their subcontractors, who believed that the DFARS clause did not apply to them. One of these contractors was more specific, noting that many of its suppliers believe that the DFARS clause only flows down to subcontractors covered by the cost accounting standards. In follow-up, the contractor stated that the contract language is generally clear about the requirements for suppliers, but that the focus on prime contractors covered by cost accounting standards can be misleading. Another contractor noted that it had experienced few changes implementing these requirements with its subcontractors, but that it believed other prime contractors and DOD program offices have interpreted the flowdown clause to require the prime to personally review the subcontractor's plan for the detection and avoidance of counterfeit electronic parts, independent of DCMA review.

In addition to confusion associated with flowing down the counterfeit electronic parts requirements to subcontractors, the contractors we spoke with raised some concerns about the coverage of the DFARS counterfeit electronic parts clause requirement. In one context, they expressed concern that gaps in the coverage of the counterfeit parts requirements might be increasing the risk of introducing counterfeit electronic parts in the DOD supply chain. Two contractors stated that the risk of counterfeit parts is largely associated with suppliers that are not covered by cost accounting standards, and that although flowing down these requirements from prime contractors addresses some of this risk, many equally risky subcontractors are suppliers to prime contractors that are not covered by cost accounting standards and therefore are not subject to the DFARS clause or its requirement to flow it down to subcontractors. However, some contractors noted that commercial suppliers, who the prime contractors consider low-risk, may refrain from working with the government because of these requirements. These contractors told us that the DFARS requirements increase the difficulty of working with commercial suppliers, for whom government contracts represent a small percentage of their overall revenue. They further stated that the costs and

burdens of implementing DOD's Counterfeit Prevention Policy, particularly for commercial-off-the-shelf items, outweigh the potential sales to government.

DOD Counterfeit Detection Efforts Include Improving Testing and Traceability, Collaborating with Other Agencies, and Improving Purchasing Processes

In addition to reporting to GIDEP, DOD and the defense industry have adopted and are developing additional methods to detect and avoid counterfeit parts from entering the DOD supply chain systems. They are working to improve testing to detect counterfeit parts, implementing tools to improve the traceability of electronic parts, sharing information with other government agencies, and improving purchasing processes. These counterfeit detection efforts are critical when the option to procure parts from an authorized source is not available. DOD policies and regulations, and international standards, document the importance of detection efforts, such as testing and authenticating parts, but emphasize that purchasing parts directly from an original component manufacturer or authorized supplier, whenever possible, is the best strategy to avoid counterfeit parts. According to a few officials from the defense industry and DOD, despite the challenges in adopting effective practices and methods to detect counterfeit parts in the U.S. defense supply chain, they are ahead of other countries and international companies in addressing this issue.

Industry and Government Are Making Improvements to Counterfeit Testing

Industry and government are working collaboratively, as part of an international committee to develop uniform standards for testing counterfeit electronic parts. In 2010, SAE International, an organization that develops international standards for the aerospace and automotive industry, established a subcommittee to develop uniform test method standards for detecting counterfeit electrical, electronic, and electromechanical (electronic) parts. This subcommittee is part of the broader SAE International G-19 committee that previously issued broader standards addressing the risk of counterfeit parts. Representatives of the committee include officials from DOD agencies such as DLA and the Navy, defense contractors, test labs, industry groups, and academia.

According to SAE International, its testing standard will include guidance for determining a part's counterfeit risk, as well as separate documents initially addressing a combination of ten specific test methods for various types of electronic parts counterfeiting. The types of tests include external visual inspection, radiological inspection, x-ray fluorescence, and electrical testing. Once the guidance is issued, it is intended to be applied across the supply chain to include independent testing facilities, distributors and original equipment manufacturers with in-house testing

capabilities, and other prime contractors or high-level subcontractors that can flow down the test requirements to their subcontractors. The committee plans to finalize the standard in 2016.

The defense industry has also led efforts to evaluate and improve the quality of testing of suspect counterfeit parts performed by industry, government, and university labs. To address industry and government concerns about testing quality, one prime contractor developed a series of "round robin" tests for labs to compare and assess the quality of their testing with other labs. For the assessment, the contractor sent samples of defective parts to both the contractor's internal testing facilities and independent labs where it outsources testing to determine their accuracy in identifying counterfeit parts. After the test results are compiled, participants receive their results along with other participants' results for comparison, though the names of the other participants are kept confidential. The testing program has expanded to include commercial test labs, contractor in-house labs, distributor in-house labs, government labs, and university labs. The results of these evaluations of testing facilities have been presented to the G-19 committee to inform the development of its test methods standard for counterfeit parts. In addition, NASA officials said that their labs have participated in the round robin testing as part of their efforts to maximize their in-house counterfeit testing capabilities, due to a lack of confidence in external test labs.

DOD Maintains Internal Testing Capabilities to Detect Evolving Threat of Counterfeit Parts

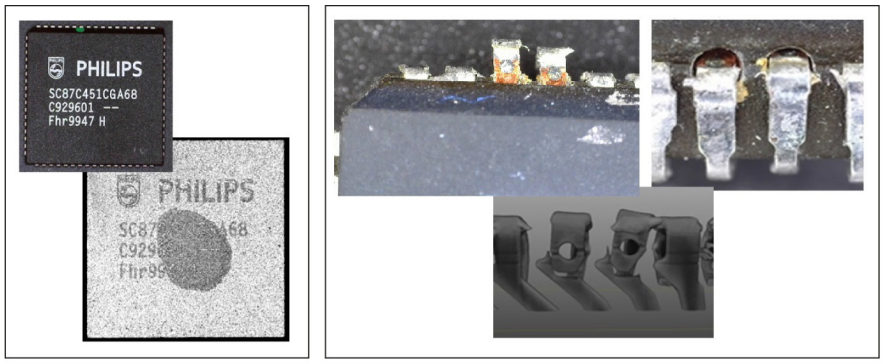
To support DOD's counterfeit detection efforts, DLA has internal testing capabilities to detect counterfeit parts purchased across the DOD. DLA is responsible for purchasing replacement and support parts for the services, including providing over 90 percent of the military's repair parts, and views that its counterfeit prevention efforts have a critical role in preventing counterfeit parts from entering DOD systems during operations and support phase of a system. To test these parts for quality issues and non-conformances, including testing for suspect counterfeit parts; DLA has product test centers at two locations to conduct three types of tests: mechanical; electronic; and analytical and chemical. DLA's test centers conducts about 13,000 tests a year and have completed over 58,000 total tests from fiscal years 2011 through March 2015, of which 8,925 were specifically for electronic parts. DLA test results do not specifically categorize negative test results as suspect counterfeit, but according to DLA officials, test results may be used for further investigation, which could result in a GIDEP report or a legal action against the supplier. DLA parts testing can be initiated for multiple reasons such as responding to a field complaint or identified discrepancy,

random stock sampling, targeted testing of specific vendors with no historical data or past poor performance, or testing of new vendors. DLA officials noted that the test centers have adopted new methods to address evidence of counterfeit parts. For example, a DLA electronic test center created a visual inspection checklist in December 2013 for testing microcircuits to identify defects that could indicate that the part had been previously used or marked, indicating tampering.

The Naval Surface Warfare Center in Crane, Indiana is another facility leading efforts to mitigate the risk of counterfeit parts. It has been providing testing and other support for preventing counterfeit parts from entering Navy systems since 2009. Naval Surface Warfare Center Crane can perform at least 24 types of electrical and physical tests to authenticate and analyze parts to detect counterfeits and has conducted investigations on over 3,000 parts. Naval Surface Warfare Center Crane works with DOD investigative agencies, the intelligence community, and suppliers to acquire and analyze newly discovered forms of counterfeiting in order to adapt new techniques. For example, Naval Surface Warfare Center officials cited an emerging threat whereby clones—exact copies of electronic parts not supplied by the original equipment manufacturer—are being reverse-engineered from stolen intellectual property. In addition to testing parts and working to identify emerging counterfeit threats, Naval Surface Warfare Center Crane, in partnership with MDA, has performed audits and assessments of over 50 independent distributors to evaluate their capabilities to detect counterfeit parts. Figure 6 shows examples of tests to detect suspect counterfeit electronic parts. In response to a provision in the 2016 National Defense Authorization Act, DOD officials noted that Naval Surface Warfare Center Crane is also conducting an assessment of the extent to which counterfeit parts are causing field have caused failures in fielded systems. This assessment is expected to be completed in 2017.[29]

[29]Section 238, FY16 NDAA, Pub. L. No. 114-92 (Nov 25, 2015).

Figure 6: Examples of Tests to Detect Suspect Counterfeit Electronic Parts



Source: Naval Surface Warfare Center Crane Division. | GAO-16-236

An acoustic microscopy test identified that the center of the part contained a different material that was otherwise undetectable upon visual inspection.

Visual inspection and X-ray revealed part leads that were replaced and covered up.

DOD Is Improving Parts' Traceability

To minimize the risk of counterfeit parts entering its supply chain, DOD is implementing steps to improve its ability to trace electronic parts back to the original manufacturer and lower supply chain levels. DLA officials told us, for example, that they validate the traceability of 100 percent of their contract awards for microcircuits by applying a botanically-derived marking to all electronic microcircuits—determined to be at a high-risk for counterfeiting—that are purchased by the agency. The marking contains tracking information about the part such as the supplier, lot number, and other identification codes, which can all be retrieved with a hand scanner at any point throughout its serviceable life. DLA places the markings on the surface of the microcircuits at a single facility once it is inspected and its trace documentations authenticating its origin with the original component manufacturer are confirmed. According to DLA officials, DLA applies the marking to about 85,000 microcircuits a year, and is exploring the possibility of expanding the program to other parts that are at high-risk for counterfeiting.

The Defense Advanced Research Projects Agency is also developing a system to authenticate and track electronic parts throughout the supply chain. The Supply Chain Hardware Integrity for Electronics Defense program is developing a microscopic computer chip, which unlike DLA's marking program, will be inserted at the original source of the part and, according to contractor officials, would further strengthen authentication. The microchip will contain a unique identifier for authentication and will

record the reliability of the part through the chip's sensors and communications systems. DOD announced that the Defense Advanced Research Projects Agency awarded a development contract for the program in January 2015 and plans to transition the technology to field trials within 3 years, then to industry partners in 4 years once trials are completed. One industry official noted, however, that the success of this program depends upon the willingness of original component manufacturers to implement it.

DOD Is Collaborating with Federal Agencies to Detect Counterfeit Parts

A group of federal agencies, including DOD, are working collaboratively to improve the detection and interception of counterfeit parts in the defense supply chain. Specifically, Immigration and Customs Enforcement's Homeland Security Investigations within the Department of Homeland Security began an initiative in 2011, called Operation Chain Reaction. This initiative is led by the Department of Homeland Security's National Intellectual Property Rights Coordination Center with a mission to align federal efforts to combat the proliferation of counterfeit goods into the DOD and federal government supply chains. Sixteen federal agencies, including the Defense Criminal Investigative Service, the military investigative services, and the DLA Office of the Inspector General, as well as the Department of Energy, the NASA Office of the Inspector General, and the U.S Customs and Border Protection are participating in the initiative. Operation Chain Reaction's partnership has had several actions that resulted in detections and seizures of counterfeit parts, including one that resulted in the October 2015 sentencing of a man who imported thousands of counterfeit integrated circuits from China and Hong Kong to resell them to U.S. customers, including contractors supplying them to the U.S. Navy for use in nuclear submarines. Moreover, in fiscal year 2015, Operation Chain Reaction initiated a pilot program with DLA to validate its current counterfeits prevention practices. By sharing information about DLA inventory with the original manufacturers, this program helps to identify counterfeits in DLA's current supply and evaluate newly ordered parts for authenticity.

DOD is Modifying Its Purchasing Processes to Mitigate Counterfeit Risk

As the largest purchaser of electronic parts in DOD, DLA has developed two supplier lists for circumstances in which a part may not be available from an authorized source. In 2009, DLA responded to the risk of counterfeit electronic parts by developing the Qualified Suppliers List of Distributors for companies that sell semiconductors and microcircuits. To be listed, suppliers must meet DLA standards for traceability to the original component manufacturer and part reliability. For instances in

which a DLA buyer cannot source a supplier with appropriate authentication credentials or traceability no longer exists, DLA created the Qualified Testing Suppliers List of semiconductor and microcircuit suppliers in 2012 that meet DLA-approved testing and other quality assurance standards for the parts. All listed suppliers must meet criteria established by DLA and be subject to onsite audits. Once approved for either program, participants can be subject to random site audits, and are audited on a regular basis. According to DLA officials, these audits can occur every 2 to 5 years, based on the perceived risk of the supplier. These lists have 39 and 20 suppliers respectively. A senior DLA official noted that the development of these lists has allowed DLA to limit its supplier base to certain suppliers but still provide enough suppliers for sufficient competition. The official added that if DLA cannot procure these types of parts from an original component manufacturer, authorized manufacturer, or listed supplier and has to use another distributor, then the part will be subject to product verification testing.

In addition, DLA, the Navy, and the Office of the Secretary of Defense are upgrading the Past Performance Information Retrieval System, which serves as a government-wide repository of contractor past performance data, to include counterfeit parts and supplier data in order to identify procurement risk. As part of the system's planned capabilities, it will serve as a repository for contractor and item risk assessments based on information from multiple sources including PDREP, GIDEP, product testing, and contractor suspension and debarment history. According to DLA and Navy officials we spoke with, this program, once implemented, will incorporate all the data for analyses and predict probabilities for the chance of a supplier to introduce counterfeit materials into the supply chain. The first phase of the enhancements has already been completed to allow users to identify suppliers that have been excluded or debarred for reasons, such as selling counterfeit parts, and allows agencies to flag certain high-risk parts that have been counterfeited in the past. The program is expected to be completed by early fiscal year 2018, according to a Navy official. Initially, DOD will have sole access to the new system, but according to DOD officials, future planned enhancements may include providing access to other federal agencies.

Conclusions

The DOD supply chain is vulnerable to the risk of counterfeit parts—which can have serious consequences. To effectively identify and mitigate this risk, DOD and its defense contractors need data on the existence of counterfeit parts in their supply chain; whether those be suspected or confirmed counterfeit. Three years after GIDEP reporting became

mandatory, we found evidence that this system may not be effective as an early warning system to prevent counterfeit parts from entering the supply chain. Without proper oversight to ensure the reporting requirement is consistently applied, DOD cannot depend on GIDEP data to ensure it is effectively managing the risks associated with counterfeit parts. DOD's lack of insight into DLA's reporting practices is particularly problematic, given DLA's key role in procuring parts for the department. Further, without a standardized process for establishing the level of evidence needed to submit suspect counterfeit GIDEP reports, defense agencies—particularly DLA—and contractors have demonstrated a reluctance to report suspect parts, creating a delay in knowledge-sharing and an opportunity for counterfeit parts to be used in defense products. Also, DOD needs to be sure that information in GIDEP about suspect counterfeit parts is reaching industry participants whenever possible, but currently lacks necessary guidance to ensure this occurs.

In addition, DOD relies on its prime contractors and subcontractors to have systems in place to detect and avoid counterfeit parts, but DOD has not yet clarified for industry the criteria by which it will assess and monitor those systems. Without providing further clarification about the criteria against which they will be evaluated, DOD cannot effectively empower its prime contractors and subcontractors to perform their critical role in consistently protecting the supply chain from counterfeit parts. Moreover, recent efforts by DOD and the defense industry to improve part traceability and testing are taking shape, but these efforts cannot be appropriately targeted to the greatest risk vulnerabilities without complete data on the existence of counterfeit parts.

Recommendations for Executive Action

To provide greater compliance with the GIDEP reporting requirement among the DOD components and their defense supplier-base, we recommend that the Undersecretary of Defense for Acquisition, Technology and Logistics take the following three steps:

- Establish mechanisms for department-wide oversight of defense agencies' compliance with the GIDEP reporting requirement.
- Develop a standardized process for determining the level of evidence needed to report a part as suspect counterfeit in GIDEP, such as a tiered reporting structure in GIDEP that provides an indication of where the suspect part is in the process of being assessed.

- Develop guidance for when access to GIDEP reports should be limited to only government users or made available to industry.

To help DOD and contractors to have a greater degree of certainty and consistency to adhere to the requirements for contractor counterfeit detection and avoidance systems, we recommend that the Undersecretary of Defense for Acquisition, Technology and Logistics:

- Clarify for industry the criteria by which DOD will assess contractor counterfeit detection and avoidance systems.

Agency Comments and Our Evaluation

We provided a draft copy of this report to the Departments of Defense, Energy, Homeland Security, Justice, and Transportation; as well as the Administrator of the National Aeronautics and Space Administration for their comment. In written comments, DOD concurred with our three recommendations directed at providing greater compliance with the GIDEP reporting requirement among the DOD components and their defense supplier-base. Specifically, DOD plans to issue a new Instruction on GIDEP in fiscal year 2017, covering the identification of roles and responsibilities for submitting GIDEP reports and oversight; the level of evidence needed to report a part as suspect counterfeit in GIDEP; and the use of GIDEP, including guidance for when access to GIDEP reports should be restricted to government only. DOD partially concurred with our recommendation aimed at helping DOD and its contractors to have a greater degree of certainty and consistency to adhere to the requirements for contractor counterfeit detection and avoidance systems. Specifically, DOD stated that it agrees with informing contractors on how their counterfeit detection and avoidance systems will be assessed; however, it does not agree with prescribing specific counterfeit detection and avoidance system implementation details. We continue to believe it is important that DOD strengthen its communication with the contractors and as our recommendation indicated, for DOD to clarify the criteria by which it will assess contractor's counterfeit detection and avoidance systems —which is different than providing specific implementation details. *Standards for Internal Control in the Federal Government* state that for an entity to run and control its operations, it must have relevant, reliable and timely communication related to internal and external events, which includes providing relevant and reliable criteria to contractors so that they can appropriately develop or improve their systems to detect and avoid counterfeit parts in order for them to be determined sufficient by DOD. Providing these criteria allows contractors greater visibility into DOD's expectations. DOD also provided technical comments, which we

incorporated as appropriate. DOD's written comments are reprinted in appendix III.

The Departments of Energy, Homeland Security, and the National Aeronautics and Space Administration provided technical comments, which we incorporated as appropriate. The Departments of Justice and Transportation did not provide comments for this review.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Defense, Energy, Homeland Security, and Transportation; the Attorney General of the United States; the Administrator of the National Aeronautics and Space Administration; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-4841 or by e-mail at makm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.

Marie A. Mak
Director, Acquisition and Sourcing Management

List of Congressional Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Thad Cochran
Chairman
The Honorable Richard J. Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Rodney Frelinghuysen
Chairman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The report focuses on reporting of counterfeit parts and the detection and avoidance of counterfeit parts in the Department of Defense (DOD) supply chain. Specifically, our objectives were to determine (1) the use of the Government-Industry Data Exchange Program (GIDEP) to report suspect counterfeit parts, from fiscal years 2011 through 2015; (2) the effectiveness of GIDEP reporting as an early warning system for counterfeit parts; (3) the extent to which DOD has assessed defense contractors' systems for detecting and avoiding counterfeit parts; and (4) key ongoing efforts by selected government and industry organizations to improve the detection and reporting of counterfeit or suspect counterfeit parts.

We met with DOD officials and reviewed counterfeit mitigation policies and procedures from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) Logistic and Materiel Readiness, Supply Chain Integration and USD AT&L Defense Procurement and Acquisition Policy, as well as the military services and other DOD components including the Departments of the Army, Navy, and Air Force, the Missile Defense Agency (MDA), Defense Logistics Agency (DLA), Defense Contract Management Agency (DCMA), and the Defense Criminal Investigative Service. We then assessed DOD's policies, procedures and practices against criteria in *Standards for Internal Control in the Federal Government*.[1]

To determine use of GIDEP to report suspect counterfeit parts over the last 5 fiscal years, we obtained the complete GIDEP database for reports entered between October 1, 2010 and September 30, 2015. We analyzed the data to identify GIDEP reports that were categorized as suspect counterfeit and determine trends in reporting by fiscal year and across entities who submitted the reports. We assessed GIDEP by reviewing documentation and meeting with GIDEP officials, and determined that the data were sufficiently reliable for our purposes. To understand the trends in GIDEP reporting, we interviewed Air Force, Army, DCMA, DLA, MDA, and Navy officials as well as representatives from selected defense contractors and industry associations.

[1]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

To assess the effectiveness of GIDEP reporting as an early warning system for counterfeit parts, we interviewed Air Force, Army, USD AT&L, DCMA, DLA, MDA, and Navy officials as well as representatives from selected defense contractors and industry associations. In addition, we analyzed data in DOD's Product Data Reporting and Evaluation Program (PDREP) submitted between October 2010 and August 2015, the most complete data available when we conducted this analysis, to identify product quality reports coded as suspect counterfeit and assess the extent to which these reports overlapped with GIDEP suspect counterfeit reports. We assessed the PDREP data by reviewing documentation and meeting with PDREP officials, and determined that the data were sufficiently reliable for our purposes. Further, we met with officials from the Defense Criminal Investigative Service and the Department of Justice to discuss how ongoing criminal cases may impact timely GIDEP reporting.

To assess the extent to which DOD has assessed defense contractors' systems for detecting and avoiding counterfeit parts, we reviewed Section 818 of the 2012 National Defense Authorization Act, the Federal Acquisition Regulation (FAR), and the Defense Federal Acquisition Regulation Supplement (DFARS) related to detecting, reporting, and mitigating counterfeit electronic parts in the DOD supply chain by defense contractors.[2] We reviewed documents and spoke with officials at DCMA regarding DCMA's process and criteria for determining the sufficiency of contractors' systems to detect and avoid counterfeit electronic parts. We interviewed seven major defense contractors with awards containing DFARS counterfeit electronic parts language to discuss and examine their policies to detect and avoid counterfeit parts—BAE Systems, Boeing, General Dynamics, Lockheed Martin, Northrop Grumman, Raytheon, and Sikorsky Aircraft. To select these contractors, we obtained data from Defense Procurement Acquisition Policy identifying all 2014 DOD awards and contract actions containing the DFARS counterfeit electronic parts language and selected the five contractors with the largest dollar value of such actions, as well as two other contractors with smaller, but still significant, total volume. Additionally, for each of these

[2]DFARS §§ 231.205-71, 244.303, 244.305-71, 246.870-1, 246.870-2, 246.870-3, 252.244-7001, and 252.246-7007; for proposed FAR amendments, see 79 Federal Register 33164 (June 10, 2014), proposing amendments to FAR §§ 2.101, 7.105, 12.208, 12.301, 46.101, 46.102, 46.105, 46.202-1, 46.317, 46.407, 52.213-4, 52.244-6, and a new clause at 52.246-XX.

contractors, we non-judgmentally selected one contract from the 2014 dataset, covering a range of award values and products and services, to examine how DOD counterfeit parts requirements for contractors are applied in a variety of situations. In addition, we met with industry associations representing companies from various levels of the defense industry supply chain, including the Aerospace Industry Association, Semiconductor Industry Association, and the Independent Distributors of Electronics Association to determine how and to what extent they worked with DOD to implement to federal regulations for counterfeit mitigation and the impact of regulations related to the detection and avoidance of counterfeit electronic parts

To identify key ongoing efforts by selected government and industry organizations to improve the detection and reporting of counterfeit or suspect counterfeit parts, we reviewed documents and data and contacted officials from Defense agencies, including Defense Advanced Research Products Agency, DLA Headquarters, and DLA Land and Maritime, as well as other government agencies, such as the National Aeronautics and Space Administration, the Department of Energy, Department of Homeland Security, and the Department of Transportation. We also obtained documents and met with representatives from SAE International and the G-19 Counterfeit Electronic Parts Committee to gain an understanding of the standards and practices being developed to detect and avoid counterfeit parts. We also met with selected defense contractors to discuss actions taken to improve their practices to detect and avoid counterfeit parts, as well as reviewed data and interviewed a representative from ERAI, related to the reporting of potential counterfeit parts. In addition, we visited the product testing facilities at DLA Land and Maritime in Columbus, Ohio and the Naval Surface Warfare Center in Crane, Indiana. In addition, we met with representatives from the Center for Advanced Life Cycle Engineering and attended a symposium about counterfeit parts and materials organized by the Center for Advanced Life Cycle Engineering and the Surface Mount Technology Association in College Park, MD.

We conducted this performance audit from January 2015 to February 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Number of Government-Industry Data Exchange Program (GIDEP) Reports by Role in Supply Chain of Entity Submitting Report (Fiscal Years 2011-2015)

Report Submitter Type	2011	2012	2013	2014	2015	Total Reports
Contractor Category						
Test Lab	72	0	0	0	0	**72**
Original Equipment Manufacturers	27	76	26	25	24	**178**
Authorized Distributors	2	0	0	1	0	**3**
Independent Distributors	152	15	16	10	14	**207**
Midlevel Manufacturers	6	7	3	5	0	**21**
Original Component Manufacturers	0	2	0	0	0	**2**
Contractor subtotal	259	100	45	41	38	**483**
Government Agency						
Defense: Navy	1[a]	19	0	1	3	**24**
Defense: DLA	0	5	3	0	1	**9**
Defense: DCMA	1	1	1	1	0	**4**
Defense: Defense Microelectronics Agency	0	1	1	1	0	**3**
Department of Energy	0	0	2	0	1	**3**
Government Subtotal	2	26	7	3	5	**43**
Total	**261**	**126**	**52**	**44**	**43**	**526**

Source: GAO analysis of GIDEP data and classifications of reporting entities. | GAO-16-236

Note: The GIDEP database does not have information about the roles in the supply chain of entities submitting reports. Categorization of these entities was completed by GIDEP staff based on their expertise and could not be independently verified by GAO.

[a]The Navy's GIDEP operations center entered a report in 2011 on behalf of the Consumer Product Safety Commission.

Appendix III: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

LOGISTICS AND
MATERIEL READINESS

FEB 2 2016

Ms. Marie A. Mak
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Mak:

Thank you for the opportunity to provide comments on this draft report. This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-16-236, "COUNTERFEIT PARTS: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," dated January 6, 2016 (GAO Code 100052). Detailed comments on the report recommendations are enclosed.

Sincerely,

Paul D Peters for

David J. Berteau

Enclosure:
As stated

GAO Draft Report Dated January 6, 2016
GAO-16-236 (GAO CODE 100052)

"COUNTERFEIT PARTS: DOD NEEDS TO IMPROVE REPORTING AND OVERSIGHT TO REDUCE SUPPLY CHAIN RISK"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: To provide greater compliance with the GIDEP reporting requirement among the DOD components and their defense supplier-base, the GAO recommends that the Undersecretary of Defense for Acquisition, Technology and Logistics establish mechanisms for department-wide oversight of defense agencies' compliance with the GIDEP reporting requirement.

DoD RESPONSE: Concur. A new DoD Instruction covering the use of GIDEP, to include identification of roles and responsibilities for submission of reports and oversight of such submission, will be issued. Development, coordination, and issuance of the new instruction are expected to be complete by the end of second quarter, fiscal year 2017.

RECOMMENDATION 2: To provide greater compliance with the GIDEP reporting requirement among the DOD components and their defense supplier-base, the GAO recommends that the Undersecretary of Defense for Acquisition, Technology and Logistics develop a standardized process for determining the level of evidence needed to report a part as suspect counterfeit in GIDEP, such as a tiered reporting structure in GIDEP that provides an indication of where the suspect part is in the process of being assessed.

DoD RESPONSE: Concur. A new DoD Instruction covering the use of GIDEP, to include the level of evidence needed to report a part as suspect counterfeit in GIDEP, will be issued. Development, coordination, and issuance of the new instruction are expected to be complete by the end of second quarter, fiscal year 2017.

RECOMMENDATION 3: To provide greater compliance with the GIDEP reporting requirement among the DOD components and their defense supplier-base, the GAO recommends that the Undersecretary of Defense for Acquisition, Technology and Logistics develop guidance for when access to GIDEP reports should be limited to only government users or made available to industry.

DoD RESPONSE: Concur. A new DoD Instruction covering the use of GIDEP, to include guidance for when access to GIDEP reports should be restricted to government only, will be issued. Development, coordination, and issuance of the new instruction are expected to be complete by the end of second quarter, fiscal year 2017.

RECOMMENDATION 4: To help DOD and contractors to have a greater degree of certainty and consistency to adhere to the requirements for contractor counterfeit detection and avoidance systems, the GAO recommends that the Undersecretary of Defense for Acquisition, Technology and Logistics clarify for industry the criteria by which DOD will assess contractor counterfeit detection and avoidance systems.

DoD RESPONSE: Partially concur.

DoD concurs with informing contractors on how their counterfeit detection and avoidance systems will be assessed. DCMA published DCMA INST-1205 Counterfeit Mitigation on July 6, 2015. This instruction is available on a public website at http://www.dcma.mil/policy/1205/DCMA-INST-1205.pdf. Additionally, DCMA provides copies of the DCMA Counterfeit Checklist and DCMA Counterfeit Mitigation Training to contractors when requested. DCMA will continue to update the Counterfeit Checklist as part of its standard operating procedures.

DoD non-concurs with prescribing specific counterfeit detection and avoidance system implementation details. The clause at DFARS 252.246-7007(c) "System Criteria" was intentionally written to allow contractors the flexibility to implement counterfeit prevention capabilities consistent with their business operations, and to leverage the evolving nature of industry standards and best practices.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Marie A. Mak, (202) 512-4841, or MakM@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Lisa Gardner (Assistant Director), Virginia Chanley, Alexandra Dew Silva, Cynthia Grant, Kurt Gurka, Stephanie Gustafson, Ashley Orr, Scott Purdy, Matt Shaffer, Roxanna Sun, and Robert Swierczek made key contributions to this report.